

EXHIBIT 36

Email attachment excerpted and formatted for legibility

From: Campbell, Danielle [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=BF58A9FD896640A592DDD2AF5D6DA453-CAMPBELL, D]
Sent: 3/2/2020 9:11:47 PM
To: Ensminger, Sandy [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=05e9c9c023b449b794de995f6362b10d-Ensminger,]; Day, Chris [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=aa9a0d2c87114c0898a128020a311291-Day, Chris]; Wehrmann, August [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=73ef7e48062645d5be3af7b9068c1f15-Wehrmann, A]; Kemmerer, Joel [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=7001182857294219b50223772a1dd507-Kemmerer, J]; Owens, David [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a4c0c534892740c8b2af623237debff0-Owens, Davi]
CC: Johnson, Rani [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0ee57945f15e47b3abaa99a59170ad3f-Johnson, Ra]
Subject: SOX: Control Deficiencies FY19
Attachments: FY2019 Deficiencies and Recommendations - Final.xlsx

Hi –

I wanted to send you an email to let you know that we have control deficiencies from our FY19 SOX Audit that will need to be remediated by your teams. I have set up meetings with the control owners over the next couple of weeks. The goal of these meetings will be to determine what remediation steps will be taken and how quickly they can be put in place. I believe that most of the remediation efforts will be around re-training the teams on the process that should be followed for financially impacting changes. I don't believe that there will need to be any work around these unless the teams decide the old process will not work and need to be changed.

Attached is a summary of all the control deficiencies for both business and IT controls. There were 20 controls that were not remediated by yearend. I would like to have all of these remediated in Q1 or early Q2. If you filter on column K, the focus will be on those that have not been remediated yet. Majority of the teams are already aware of these since they were heavily involved in the discussions with Internal Audit and PwC. Just in case they did not make it to you, I wanted to present them to you. (the IT controls are on the last tab)

Area of Testing	# of Controls Tested	Total Control Deficiencies	Remediated	Not Remediated
Business Controls	300	28	18	10
IT General Controls	100	27	17	10
Total	400	55	35	20

- ✓ Great appreciation for discipline
- ✓ Buy-in from Management and Executives
- ✓ Successfully utilized AuditBoard for internal and external audit

- Room for process improvement
- Re-training on areas of focus / high risk
- Lack of useful technology to automate
- Work in synergy with process owners

We have the Security & Compliance Quarterly Risk Review (QRR) meeting tomorrow with Jason Bliss and Bart Kalsu. We have a couple slides dedicated to the SOX findings. I did not want it to be a surprise to you that these are included in that discussion.

Please let me know if you have any questions or if you would like for me to have a separate call with you to review. I have already included you on the meeting invites with your teams to review these as well.

Overall, for our first year as a public company, I believe the teams did a good job. However, we do have areas for improvement around these controls.

Thanks,



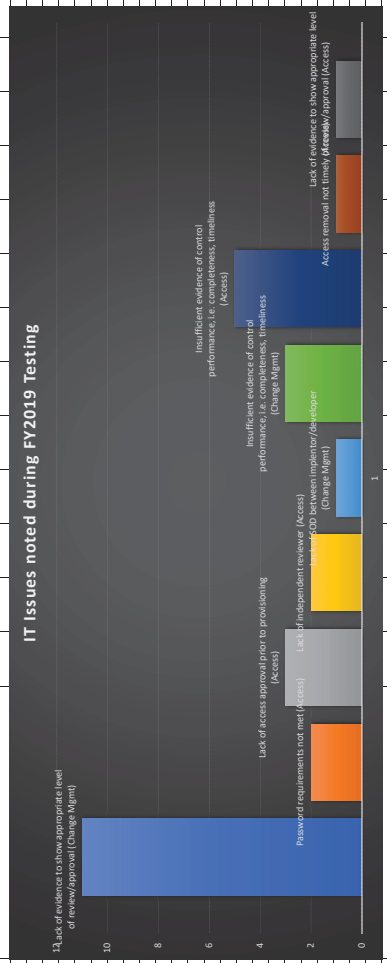
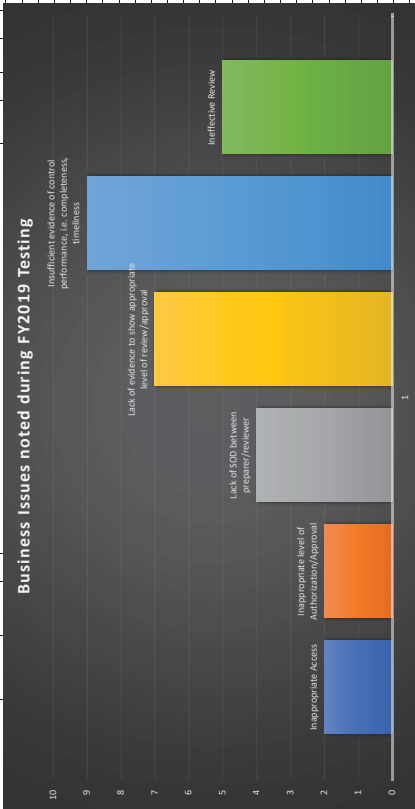
Danielle Campbell | Director of Internal Audit

Office: 512.874.3389 | Mobile: 972.467.8926

DOCUMENT PRODUCED IN NATIVE FORMAT

Summary

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	Process	# of Exceptions	SWNA	Int'l		SWNA	Int'l	Total	%			IT General Controls	Total												
1																									
2	Quinto to Cash	5	3		Inappropriate Access	1	1	2	7%			Lack of evidence to show appropriate level of review	11												
3					Inappropriate level of Authorization/Approval	2	0	2	7%			Password requirements not met (Access)	2												
4	Procure to Pay	1	0		Lack of SOD between preparer/reviewer	4	0	4	14%			Lack of access approval prior to provisioning (Access)	3												
5	Payroll	3	0		Lack of evidence to show appropriate level of review/approval	7	0	7	24%			Lack of independent reviewer (Access)	2												
6	Prepays and Accruals	4	0		Insufficient evidence of control performance, i.e. completeness, timeliness	9	0	9	31%			Lack of SOD between implementor/developer (Change Mgmt)	1												
7	Equity	5	0		Ineffective Review	3	2	5	17%			Insufficient evidence of control performance, i.e. com	3												
8	Financial Statement Close	4	0			26	3	29				Insufficient evidence of control performance, i.e. com	5												
9	Entity Level	4	0			0	0	0				Access removal not timely (Access)	1												
10												Lack of evidence to show appropriate level of review	1												
11													29												
12																									
13																									
14																									
15																									
16																									
17																									
18																									
19																									
20																									
21																									
22																									
23																									
24																									
25																									
26																									
27																									
28																									
29																									
30																									
31																									
32																									
33																									
34																									
35																									
36																									



IT Deficiencies

	A	B	C	D	E	F	G	H	I	J	K	L	M
	#	System	Process	Control Number	Control Language	Issue Short Name	Description of Control Deviation Identified by IA	Exception Type (MM, SS, CC)	Remediated Y/N	Why this impact is not pervasive?			
7		Backup	User Access Management	2.1	The Company maintains a password requirement for all financially significant systems and databases, including the requirement that they be changed periodically, meet minimum length requirements, retain password history, and require password complexity, as allowed by the application, system, or database. Web-based applications may not require active directory password requirements to be met - (1) complexity is enabled and (2) minimum password requirements are met - (3) a minimum password age is not configured as required, nor is (4) a password history requirement.	Password requirements not met (Access)	Backup appears to utilize TUL / AD first and foremost. However, application guidance notes that, in instances where TUL / AD is not a possibility, the application-specific password requirements are met - (1) complexity is enabled and (2) minimum password requirements are met - (3) a minimum password age is not configured as required, nor is (4) a password history requirement.	CC	N	The primary access path for Backup is through TUL / AD. Instances in which users are logging in outside of TUL / AD is not nearly as common and thus plays a role in limiting the risk found in the exception. Additionally, the application-specific password configuration detail meets some of the requirements, but not all, meaning there is security in the application-specific password detail not just to the extent that the control language requires. Lastly, the quarterly user access review performed over IBM provides comfort over restricted access.			
8		Backup	Access Provisioning	2.2	New users are provisioned access in accordance with the SolarWinds System Groups Matrix, require approval from manager, IT and/or the system owner. Additional Metasides to require worldwide financial results requires approval by the Financial Controller or the VP of WWF Finance.	Lack of access approval prior to provisioning (Access)	1 user (Doris Sawicki) of 8 samples that was not approved for new access	CC	Y	Despite the lack of support evidencing proper access approval prior to provisioning, any form of inappropriate access would ultimately be identified through the quarterly user access reviews performed by management per system.			
9		Backup	User Access Management	2.5	User access privileges are re-validated on a quarterly basis to confirm that users maintain appropriate access. These validation procedures are performed for all financially significant applications, systems (including Active Directory user) and databases.	Lack of independent reviewer (Access)	Management Prerequisites noted the review was performed by Igor Luchitski, Manager Operations Engineering. As Igor has privileged / write access to numerous layers within the system, it would be expected that a secondary reviewer without privileged access would also perform a review. As such, this is considered an exception.	CC	Y	The quarterly review acts as a catch of related to controls 2.2.3, 2.2.3, and 2.4. However, if those controls are performed correctly, access provisioning, access termination, and transfer access removal, this limits the potential for widespread issues resulting from the missed review of a specific database. As it relates to this specific exception, control 2.2.3 access provisioning would theoretically act as a mitigating control as a way to ensure proper access changes are granted appropriately. Assuming that control is functioning as expected, the risk of a privileged user performing a quarterly review without a secondary reviewer would be reduced.			
11		N-Active	Access Provisioning	2.2	New users are provisioned access in accordance with the SolarWinds System Groups Matrix, require approval from manager, IT and/or the system owner. Additional Metasides to require worldwide financial results requires approval by the Financial Controller or the VP of WWF Finance.	Lack of access approval prior to provisioning (Access)	2 users (Zakarya Weatherburne and Moshing Liu) of 30 samples did not have sufficient evidence of approval for their access prior to provisioning.	CC	Y	Despite the lack of support evidencing proper access approval prior to provisioning, any form of inappropriate access would ultimately be identified through the quarterly user access reviews performed per system.			
12		N-Active	User Access Management	2.5	User access privileges are re-validated on a quarterly basis to confirm that users maintain appropriate access. These validation procedures are performed for all financially significant applications, systems (including Active Directory user) and databases.	Lack of independent reviewer (Access)	Helpdesk Personnel noted the review was performed by Tim Drury, Manager Systems Engineering. As Tim has privileged / write access to numerous layers within the system, it would be expected that a secondary reviewer without privileged access would also perform a review. As such, this is considered an exception.	CC	N	The quarterly review acts as a catch of related to controls 2.2.3, 2.2.3, and 2.4. However, if those controls are performed correctly, access provisioning, access termination, and transfer access removal, this limits the potential for widespread issues resulting from a privileged user performing a review without secondary review of his/her access. As it relates to this specific exception, control 2.2.3 access provisioning would theoretically act as a mitigating control as a way to ensure proper access changes are granted appropriately. Assuming that control is functioning as expected, the risk of a privileged user performing a quarterly review without a secondary reviewer would be reduced.			
15		NetSuite	Access Review	2.5	User access privileges are re-validated on a quarterly basis to confirm that users maintain appropriate access. These validation procedures are performed for all financially significant applications, systems (including Active Directory user) and databases.	Insufficient evidence of control performance, i.e. completeness, timeliness (Access)	Terminated users who appeared with active NetSuite access were not captured and requested for removal during the Q4 NetSuite user access review.	CC	N	In an effort to address the potential pervasiveness of the deficiency noted, SolarWinds management performed a full review over term terminations for the 2023 year specific to NetSuite in order to ensure this issue was not pervasive beyond what was noted in the exception language. Additionally, for the terminated employees noted within the exception language, despite the delay in access removal, management noted no user logins took place after the stated termination dates of each employee tested.			
16		NetSuite / Zora UK / Zora Canada	Terminations	2.3	When an employee is terminated, access to Active Directory and financial systems is removed in a timely manner as follows: - within 2 hours for administrative access - within 7 days for all other levels of access	Access removal not timely (Access)	3 terminated users (of 25 samples) in terminated active access in NetSuite. While AD access was tested and found to be deactivated appropriately, noted that users in NetSuite and Zora UK/Canada systems can access the application without utilizing SSO.	CC	N	While it was noted the NetSuite termination involves deficiency extended into another deficiency within the NetSuite quarterly user access review, SolarWinds management performed a full review over terminations for the 2023 year specific to NetSuite in order to ensure the issue was not pervasive beyond what was noted in the exception language. Additionally, for the terminated employees noted within the exception language, despite the delay in access removal, management noted no user login took place after the stated termination dates of each employee per last test.			
17													
18													
19		Orchestration / Updater / Connector	Access Review	2.5	User access privileges are re-validated on a quarterly basis to confirm that users maintain appropriate access. These validation procedures are performed for all financially significant applications, systems (including Active Directory user) and databases.	Insufficient evidence of control performance, i.e. completeness, timeliness (Access)	The Q3 2019 Net User Operations Review was performed by John Matthews, Senior Operations Manager, on 7/10/2019. However, it was noted that there was no evidence of John performing a full review. John's electronic signature was missing for the review over the TFS/SQL database. Additionally, so was noted in the Q3 2019 review that the application teams following implementation of the HR system in October, management follow-up items was not able to be determined. Lastly, secondary review over John's access was not performed.	CC	Y	While the exception was noted during the Q3 2019 review, the issue was remediated in 2019 during the quarterly reviews that followed. Additionally, there are mitigating controls that would theoretically work to address a missed quarterly review. The quarterly review acts as a catch of related to controls 2.2.3, 2.2.3, and 2.4. However, if those controls are performed correctly, access provisioning, access termination, and transfer access removal, this limits the potential for widespread issues resulting from the missed review of a specific database.			
20		Policy	Access Policy	2	A user access management policy is established and documented for initiating, authorizing, recording, processing, reviewing a request for access rights, and evidence of retention. The policy is reviewed and approved annually by the VP of IT. Evidence of review is documented and maintained.	Lack of evidence in place (Access)	Access policy was not reviewed during FY19.	CC	N	Despite the Access policy not being reviewed by management during the 2019 year, the control detailed within the policy are active and in place among all employees relevant to the user access processes. A lack of management review of the policy document would not alter controls expected to be in place and functioning properly.			
21													
25		RMM	User Access Management	2.1	The Company maintains a password requirement for all financially significant systems and databases, including the requirement that they be changed periodically, meet minimum length requirements, retain password history, and require password complexity, as allowed by the application, system, or database. Web-based applications may not require active directory password requirements to be met - (1) complexity is enabled and (2) minimum password requirements are met - (3) a minimum password age is not configured as required, nor is (4) a password history requirement.	Password requirements not met (Access)	RMM appears to utilize TUL / AD first and foremost. However, application guidance notes that, in instances where TUL / AD is not a possibility, the application-specific password requirements are met - (1) complexity is enabled and (2) minimum password requirements are met - (3) a minimum password age is not configured as required, nor is (4) a password history requirement.	CC	N	The primary access path for RMM is through TUL / AD. Instances in which users are logging in outside of TUL / AD is not nearly as common and thus plays a role in limiting the risk found in the exception. Additionally, the application-specific password configuration detail meets some of the requirements, but not all, meaning there is security in the application-specific password detail not just to the extent that the control language requires. Lastly, the quarterly user access review performed over IBM provides comfort over restricted access.			
26		RMM	Access	2.2	New users are provisioned access in accordance with the SolarWinds System Groups Matrix, require approval from manager, IT and/or the system owner. Additional Metasides to require worldwide financial results requires approval by the Financial Controller or the VP of WWF Finance.	Lack of access approval prior to provisioning (Access)	2 users (for 34 samples) did not have evidence of appropriate approval prior to provisioning.	CC	Y	Despite the lack of support evidencing proper access approval prior to provisioning, any form of inappropriate access would ultimately be identified through the quarterly user access reviews performed per system.			

